Electronic Recording Delivery System
Baseline Requirements & Technology Standards

Addendum to the following ERDS Program Handbooks:

Vendor Software

Computer Security Auditor

System Certification

California Department of Justice

CJIS Operations Support Bureau

Electronic Recording Delivery System Program

TABLE OF CONTENTS

1 INTRODUCTION

The purpose of this document is to set the minimum baseline technology requirements and adopt architecture for the Electronic Recording Delivery System (ERDS). This technology and architecture baseline shall include interoperability standards and data standardization for digital/digitized electronic records.

2 DEFINITIONS

Term	Definitions
Acknowledge Generated	The event signaling the response of the web server.
Agent	A party designated as a representative of an Authorized Submitter (see Authorized Submitter). The agent shall not be a vendor and/or computer security auditor of electronic recording delivery systems.
Approved Escrow Company	An escrow company approved pursuant to California Code of Regulations, Title 2, beginning with section 20630.
Assemble Digital Record	The process of selection and verification of a digital document to be sent as a message to the County Recorder.
Assemble Digitized Record	The process of verifying and combining the components (digitized image, index, etc.) into a message to be sent to the County Recorder.
Assign Recorder Role	A person identified by the ERDS is assigned a specific role in the recordation process. The role provides specific privileges, dictating the level of access to the ERDS, and permissions to examine and record digital, digitized, or both documents/instruments, and communicate the results with the Submitter.
Assigned Submitter Role	A person identified by the ERDS is assigned a specific role in the recordation process. The role provides specific privileges, dictating the level of access to the ERDS, and permissions to submit digital, digitized, or both documents/instruments.
Attorney General	The Attorney General of the State of California.

Term	Definitions
Authenticate Individual	Uniquely identifies an individual attempting to use the ERDS. Every person using the ERDS regardless of his/her role in the business of recordation shall have a unique way of self-identification to the system. Unidentified people are not allowed to use the ERDS.
Authenticate Message	The process utilizing the “hash” value received with the message to validate that the received digitized or digital file was not altered during transmission.
Authorized Access	A role assigned to an Authorized Submitters who is designated to submit only digital documents to the County Recorder’s ERDS.
Authorized Submitter	An entity of the Industry (Title Insurer, Title Company, Institutional Lender) or Government (Local, State, Federal Agency) that is a party to a contract with a County Recorder to use an ERDS as a tool to electronically submit either digital/digitized instruments as designated by the County Recorder for recordation.
Authorized Submitter’s Signature	A method for authenticating digital information sent to or from the Authorized Submitter. Analogous to ordinary physical signatures on paper, but implemented using techniques from the field of public-key cryptography.
Business Processes	Workflows and processes within and between organizations outside the boundaries of the ERDS.
Certificate Authority	The certificate authority issues digital certificates for the purpose of establishing SSL sessions between Authorized Submitters and the County Recorder. The Certificate Authority also validates digital certificates presented as proof of identity.
CFE	Certified Fraud Examiner – Associated to the Association of Certified Fraud Examiners, who has at least two years of experience in the evaluation and analysis of Internet security design.
CIA	Certified Internal Auditor - Certified by the Institute of Internal Auditors.
CISA	Certified Information Systems Auditor, Certified by the Information Systems Audit and Control Association.
CISSP	Certified Information Systems Security Professional – Associated to International Information Systems Security Certification Consortium (ACFE), who has at least two years experience in the evaluation and analysis of Internet security design, the conduct of security testing procedures, and specific experience performing Internet Penetration studies.

Term	Definitions
Client	Any computer that is hooked up to a computer network.
Compiler	A program which converts high-level source language instructions into executable machine code.
Computer Security Auditor	Computer security personnel hired to perform an independent audit of the electronic recording delivery system. The computer security auditor shall be independent of the County Recorder and the Authorized Submitter and shall not be the same contractor/vendor hired to establish or participate in a county's electronic recording delivery system or in the Authorized Submitter's portion of that system.
Confirm Sender	The process of decrypting the message received to assure the identity of the sender.
County Perimeter	Perimeter security systems of counties shall include security devices configured to protect ERDS components from unauthorized activity occurring on internal or external operations. At a minimum, systems shall include a firewall and intrusion detection and/or prevention systems. Connections to ERDS made via virtual private networks shall still come under the controls provided by the perimeter security systems.
County Recorder	A public official responsible for keeping records of real estate transactions, ownership and other instruments of property rights for a County. The County Recorder shall control the assignment of roles to individuals that have access to the ERDS System.
County Recorder Examiner	A role in the County Recorder's office authorized to review electronic documents submitted for recordation.
County Recorder's Signature	A method for authenticating digital information sent to or from the County Recorder. Analogous to ordinary physical signatures on paper, but implemented using techniques from the field of public-key cryptography.
County Workstation	Contains or downloads software necessary for ERDS functions.
Deployer	Authorized to deploy approved application software to production systems.
Developer	Authorized to develop application software, but deployment is limited to the test environment.

Term	Definitions
Digital Electronic Record	Record containing information that is created, generated, sent, communicated, received, or stored by electronic means, but not created in original paper form.
Digital or Digitized Document	Documents prepared for submission.
Digital Record	A document defined in XML or XHTML that contains all the information necessary for its presentation on a screen or on paper.
Digital System	A paper based document instrument (Scanning) or electronic document – instrument previously created by a word processor or other computer program with following conversion to image.
Digitized Electronic Record	A scanned image of the original paper document.
Digitized Record	An electronic image of a document that has been generated through a process of digitization of either a paper based document-instrument (scanning), or an electronic document-instrument previously created by a word processor or other computer program with following conversion to image.
Digitized System	A system that is capable of handling (receiving, storing, and retrieving) digitized instruments i.e., document affecting a right, title, or interest of a party in a real estate property transaction, as electronic images obtained through a process of digitization of either a paper based document-instrument (scanning); or an electronic document-instrument previously created by a word processor or other computer program with following conversion to image.
Disqualifying Offenses	A felony conviction or pending charges involving offenses which will be justification for denial of secure access. A misdemeanor conviction or pending charges involving offenses which will be justification for denial of secure access.
DOJ	The California Department of Justice or any employee of the Department of Justice acting under the authority of the Department of Justice, and may be referred to as “the Department” or as “DOJ”.
DTD	Document Type Definition.
Electronic Recording Delivery System	A system to deliver for recording, and to return to the party requesting recording, digitized or digital electronic records.

Term	Definitions
Electronic Signature	Analogous to ordinary physical signatures on paper, but implemented using techniques from the field of public-key cryptography.
Electronic Signature of the Notary	A method for authenticating digital information sent to or from the Notary. Analogous to ordinary physical signatures on paper, but implemented using techniques from the field of public-key cryptography
Encrypted	Computer data and messages that have been converted into something incomprehensible using a key, so that only a holder of the matching key can reconvert them.
ERDS	Electronic Recording Delivery System.
ERDS Program	The program within the Attorney General's office, Department of Justice, responsible for the implementation of the ERDS.
ERDS Security Processes	A set of business processes implemented as a portion of the ERDS to assure confidentiality and integrity of documents while being transmitted/received via the public Internet.
ERDS Server	Receives submitted documents from the web server. Sends processed documents back to the web server.
Escrow	The process by which a third party having no direct or indirect financial interest with a vendor holds for safekeeping the source code, including all changes or modifications and new or amended versions.
Escrow Agreement	An "escrow agreement" is a contract or sub-agreement to hold each source code in escrow. The contract may be a master contract with separate sub-agreements to hold each source code in escrow or an individual contract entered into for each source code placed in escrow.
Escrow Facility	Is the physical location in which the source code and other materials may be stored for assurance of continuity of ERDS operations in case of unforeseen business troubles with the Vendor of the ERDS. No County Recorder may act as an escrow facility to store its own source code.
Examiner	A role in the County Recorder's office authorized to review electronic documents submitted for recordation.
FBI	Federal Bureau of Investigation.
GIAC System and Network Auditor	Global Information Assurance Certification for Network Auditors.

Term	Definitions
GSNA Certification	Global Systems and Network Auditor Certification.
Hardened	Hardening is the process of eliminating basic vulnerabilities on the operating system. It is a process including a setup checklist and is one of the first and most important considerations when securing a public access workstation or server. The list of possible steps that can be taken to do this is very long, and the procedure can vary for each installation environment. Furthermore, each operating system requires different steps. Hardened refers to a system and/or workstation that where a hardening process has been successfully applied.
Information Security	The data residing in the electronic recording delivery system is confidential and the use of this information for any purpose other than the purpose for which it was expressly provided is strictly prohibited. Every person as designated by a county recorder who, in the course of this normal duties collects, processes and/or facilitates the capture, development and/or transfers electronic recording delivery system data shall be required to sign an ERDS Security access and Authorized Access Statement, acknowledging that they understand their responsibilities for protecting confidential electronic recording delivery system information, the restrictions concerns the use of such information, and the penalties for misuse. Signed copies of Certification for shall be retained by the County Recorder and shall be made available to the Attorney General upon request.
Instrument Sent	The event ending the process thread of submitting the document.
Internal Network	Network used by County Recorder.
Live Scan	A system for the electronic submission of applicant fingerprints and the subsequent automated background check and response.
Local Inspection	In addition to the annual Computer Security Audit, a County Recorder and any agency or affiliated business entities shall be subject to an ERDS Local Inspection. The purpose of this inspection is to ensure that the requirements, as set forth in the oversight procedures (refer to the system certification handbook), are being adhered to for the ongoing oversight of an electronic recording delivery system.
Login Completed	An event signaling successful completion of the ERDS logon sequence. At this point the VPN/SSL session has been established, the user ID and password have been authenticated, and the Digital Signature has been confirmed. This event initiates the ERDS Security Process download.

Term	Definitions
Modification	Any change to a certified electronic recording delivery system. This includes any changes, enhancements or upgrades to the electronic recording delivery system that were not present at the time of initial certification by the Attorney General (refer to substantive modification definition).
ORI	Originating Agency Identifier
Operating System	The core software on a computer which provides the interface between its hardware (processor, peripherals, etc.), its software, and the user. Ref: http://cyber.law.harvard.edu/readinessguide/glossary.html)
Partner Network	Internal network of the Authorized Submitter organization. Use of Partner Networks for ERDS shall comply with the ERDS Baseline Requirements and Technology Standards.
Partner Perimeter	Perimeter security systems of Authorized Submitter organizations can include multiple security devices, such as firewalls, intrusion detection and/or prevention systems, virtual private network gateways, and other devices. Use of a Partner Perimeter for ERDS shall comply with the ERDS Baseline Requirements and Technology Standards.
Partner Workstation	Contains or downloads software necessary for ERDS functions.
Personnel Security	The County recorder shall maintain a current list of all personnel and/or business entities employed by and/or acting on their behalf that have been granted secure and/or authorized access to any electronic recording delivery system.
Privacy Statement	Use of Social Security Number: You are required by law to provide your Social Security Number (SSN) or your application will not be processed for ERDS Certification. The SSN is required and will be used by the Department of Justice (DOJ) for identification and verification purposes. The SSN provided on the application will not be made available for public inspection. The SSN is a standard data element included in the DOJ criminal offender record information systems as defined in Penal Code section 13125. In addition, Family Code section 17520 requires that any state Department issuing certificates to engage in an occupation shall collect the SSN of the applicant. Collection of the SSN is mandatory. Failure to provide this information will result in the rejection of your application for certification.

Term	Definitions
Quality Control	All equipment associated with the capture and transmission of electronic recording delivery systems information shall be adequately secured at all times by assuring that software upgrades (including the installation of any patches deemed necessary by the manufacture) shall be applied in a timely fashion and shall remain current.
Ready to Process	A signal to the business processes of the Submitter about the received components. This is the Recorder's response to the Submitter indicating results of recordation.
Ready to Send Response	An event signaling to the ERDS Security Processes that the message was processed, and the responding message was prepared and is ready to be sent to the Submitter.
Receive Acknowledge	The process of receiving the response of the web server and separating the acknowledge message.
Receive Acknowledgment	The process of receiving the response of the web server and separating the acknowledge message.
Receive Request	The process of accepting the request and extracting the message from the Internet transport protocol.
Recordation	A process of recording an instrument of property rights by a County Recorder.
Repudiate	To refuse to accept (reject) an unauthorized document.
Request	This event signals the beginning of the thread to read and validate the incoming message on the County Recorder's side of the ERDS.
REQUEST Unauthorized or REQUEST Corrupted	Events initiating process threads of repudiation of the incoming message.
Response Sent	The event signaling the end of the RESPONSE thread.
Revoke	The act of elimination of authorization and credentials required for access to ERDS.
Role	Specific responsibility of a person as it relates to the ERDS.
Run Message Authentication (Hash)	The process that executes a "hash" algorithm to calculate some number to assure authentic origin of the message. The number shall be sent with the message, and used by the receiver (County Recorder) to verify authenticity and integrity of the message.

Term	Definitions
SANS Institute	The most trusted and largest source for information security training. and certification in the world.
Secure Access	A role assigned to an Authorized Submitter who is designated to submit digitized documents to the County Recorder's ERDS.
Security Administrator	Authorized to configure accounts, assign roles, and issue credentials.
Security Testing	An independent security audit by a computer security auditor.
Security Violations	Any breach of security regulations, requirements, procedures or guidelines constitutes a security violation. All security violations or suspected security violations shall be immediately reported to the Attorney General. Reports of security violations shall include the date of the incident, the parties involved (if known) the nature and scope of the incident, and any actions(s) taken, Including steps to protect against future violations.
Send to Recorder	The process of setting the message in a format suitable for transmission over the Internet and submitting it as a REQUEST type of message to a web server of a County Recorder.
Send to Submitter	The process of packing the encrypted message into Internet transport protocol, addressing it to the Submitter, and sending it via Internet.
Separate Components	The process of extracting the components of the message and preparing them for further processing.
Sign with Certificate	The process of encrypting the message with a key (public or private) to indicate the source (originator) of the message.
Site Security	The site housing all hardware and software associated with the capture, development and /or transmission of electronic recording delivery system security testing and audit reports shall be adequately secured at all time to reasonably protect against theft, damage and /or unauthorized access or use by any person.
Software	"Software" generally refers to "computer programs" a collection of instructions coded according to specific rules and in a specific sequence, which tell the computer equipment what to do and when and how to do it.

Term	Definitions
Source Code	“Source code" means a program or set of programs, readable and maintainable by humans, translated or interpreted into a form that the electronic recording delivery system can execute and includes the version of a computer program in which the programmer's original programming statements are expressed in a source language (e.g. Ada, Assembler, COBOL, Fortran, Java, etc.) which must be compiled or assembled and linked into equivalent machine-executable object code, thereby resulting in an executable software program.
SSL	Secure Sockets Layer (SSL) technology secures a Web site by encrypting information and providing authentication.
Statutory Authority	Authorized by statute.
Submit Digital	An event received from a business application signaling readiness to start the thread of submission and sending of a digital document to County Recorder.
Submit Digitized	An event received from a business application signaling readiness to start the thread of assembly and submission (sending) of the digitized document to the County Recorder.
Submitted Documents	Documents retrieved from ERDS by a County Recorder.

Term	Definitions
Substantive Modifications	Any change to a certified electronic recording delivery system. This includes any changes, enhancements or upgrades to the electronic recording delivery system that were not present at the time of initial certification by the Attorney General. The following defines substantive modifications: 1. To source code – A. Modifications or changes leading to a different functional behavior of ERDS or its part (application) B. Modifications of call signatures in interfaces with purchased components C. Modifications of data structures or structural database objects (add table or add column to a table) D. Any change that require modification of deployment procedures. 2. To Compilers – A. New version of a compiler is as a substantive modification, if the existing ERDS source code cannot be compiled error free (including warnings) without changes of the source code. 3. To related software (i.e., libraries or purchased components) – A. Any change in a component or module functionality B. Any change in call signatures of modules or call interfaces 4. To an operating system - A. Any change or upgrade that relates to security settings or security policies. 5. Modifications to Systems and/or network devices – A. Any changes to the server, workstation and/or network device hardware/software configuration that impacts the ERDS. B. Any changes to the network architecture/network design as it pertains to the ERDS. Cumulative update to a new service pack level.
Suspend	Removal of all privileges of access (see Terminate).
System Administrator	Authorized to configure hardware and operating system software.
System Certification	The issuance of an approval letter and certificate regarding a County Recorder's electronic recording delivery system by DOJ, after satisfying all certification requirements.
Terminate	Removal of all privileges of access (see Suspend).

Term	Definitions
The Internet	Defined to include all other networks that are neither internal nor partner networks. Use of the Internet for ERDS shall comply with the ERDS Baseline Requirements and Technology Standards.
Uniform Index	Every Instrument recorded by a County Recorder through ERDS shall be indexed. County may decide on the content of index as required by the existing business procedures but must follow Government Code section 27257 as a mandatory minimum for ERDS of the following data fields: 1. Date Filed - Date this instrument was filed for recordation 2. Grantor - Full name of a person or organization playing the role of grantor/defendant/first party for this Instrument 3. Grantee - Full name of a person or organization playing role of the grantee/plaintiff/second party for this Instrument 4. Title - Title of the Instrument 5. Document Number - Unique document number that was assigned to the Instrument in time of recordation 6. Book - Volume in which the record of the instrument was made by the Recorder 7. Page - Page on which the record of instrument was made by the Recorder
Vendor	Any person, group, organization, company, or entity, whether or not incorporated, who sells, leases, or grants use of, with or without compensation therefore, a software program for use by jurisdictions which conduct transactions subject to these regulations. The term “vendor” includes jurisdictions which provide or maintain software programs for their own use or for the use of others.
Web Server	County server that acts as the interface to Authorized Submitters. Login occurs at the web server.

3 ERDS BOUNDARY

Existing California laws specify that the recorder of any county may, in lieu of a written paper, accept for recording a digital and/or digitized image of a recordable instrument and specified documents in digital format, as provided for in Section 27390 of the Government Code, subject to specified conditions as established by the Attorney General. The ERDS Program specifies and details these conditions in regulations. The regulations do not attempt to dictate or constrain the business process of recordation, but to assure the integrity of the electronic instruments throughout the handling and transmission processes.

The public Internet is the vehicle for delivery of instruments prepared by an Authorized Submitter and recorded by the County Recorder. The conceptual ERDS boundary is depicted in **Figure 1.**

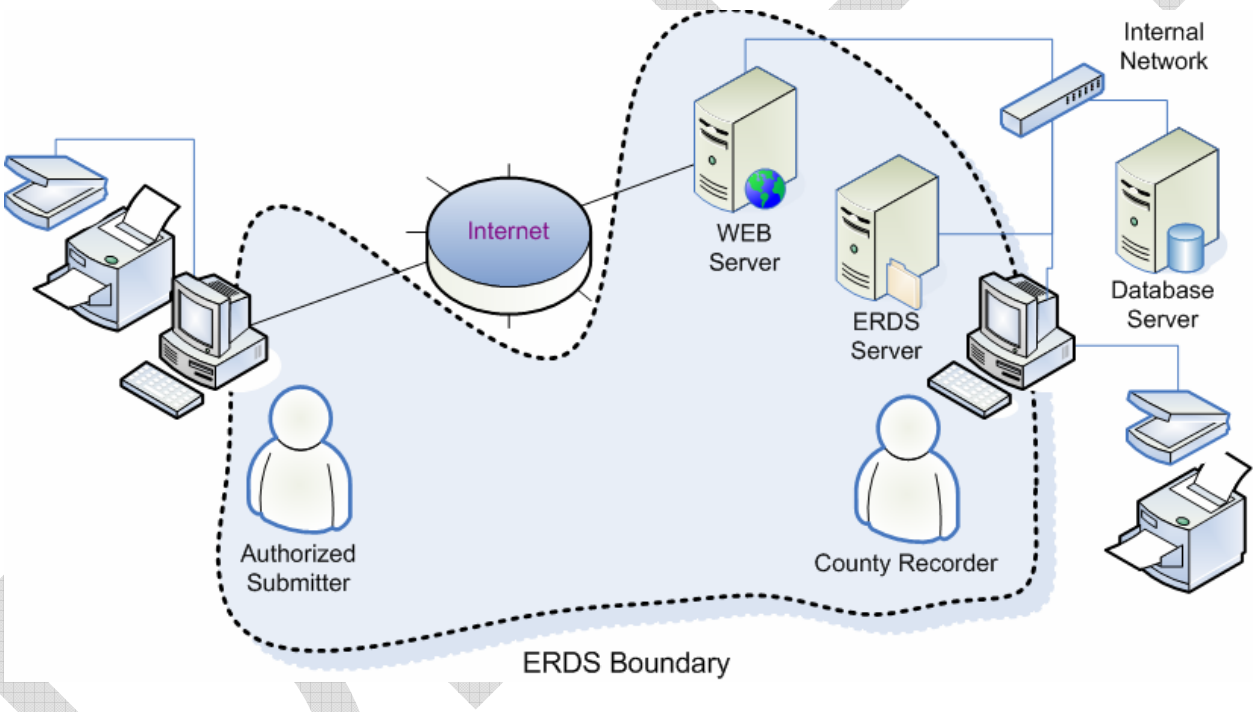

Figure 1 - ERDS Conceptual Boundary

This section sets the minimal mandatory boundaries for the ERDS.

These baseline requirements and technology standards cover provisions for confidentiality and integrity of document (message) exchange.

The ERDS is a collection of multiple workstations used by Authorized Submitters to communicate messages with the County Recorder's recordation system. When implemented, the ERDS shall have a set of modules for securing transactions over the public Internet. These processes are defined separately, for the Authorized Submitter, and for the County recordation system. **Figure 2** depicts the said processes implemented as a portion of the ERDS, hereafter referred to as the ERDS Security Processes.

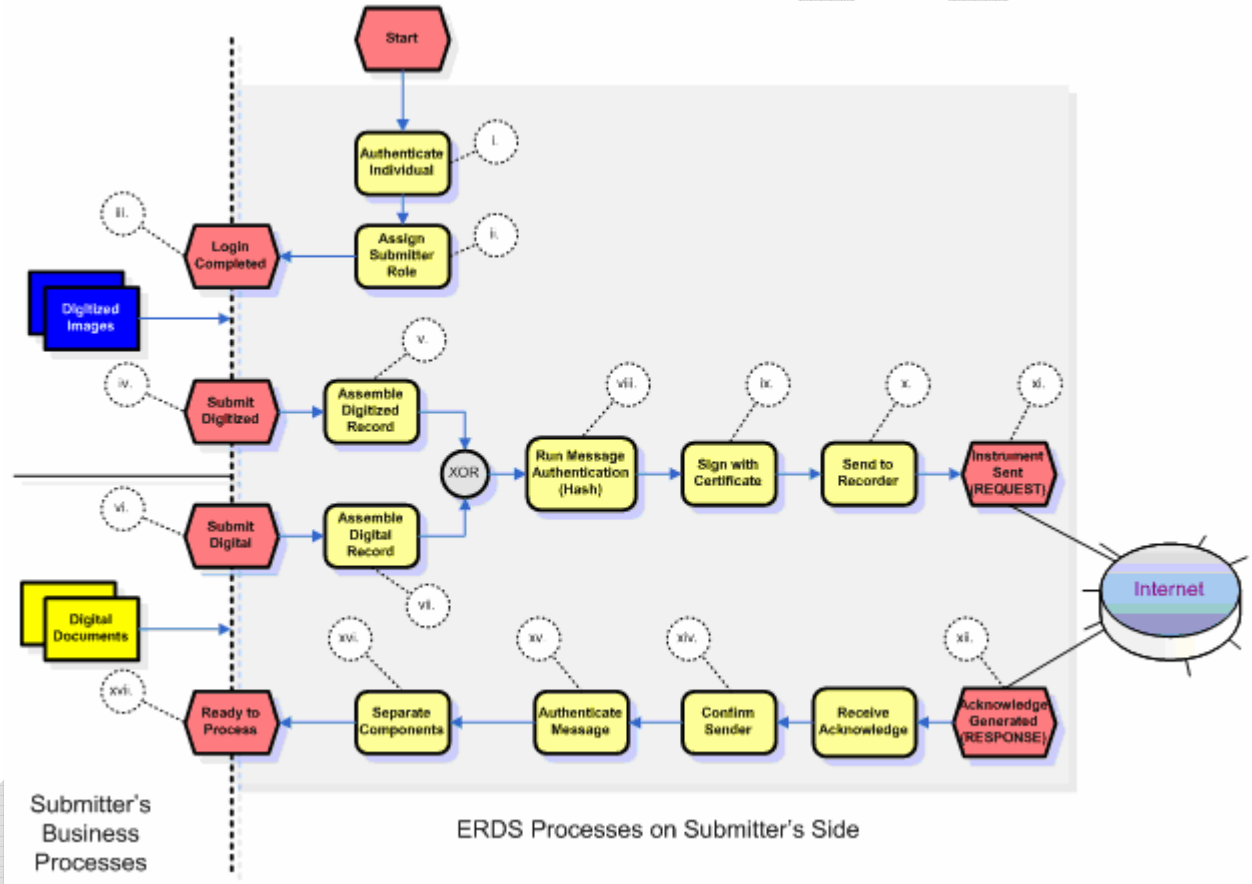

Figure 2 - **ERDS Security Processes on the Authorized Submitter's Side**

i. **Authenticate Individual** – Uniquely identifies an individual attempting to use the ERDS. Every person using the ERDS regardless of his/her role in the business of recordation shall have of unique way of self-identification to the system. Unidentified people are not allowed to use the ERDS.

ii. **Assign Authorized Submitter Role** – A person identified by the ERDS is assigned a specific role in the recordation process. The role provides specific privileges, dictating the level of access to the ERDS, and permissions to submit digital, digitized, or both documents/instruments.

iii. **Login Completed (e)** – An event signaling successful completion of the ERDS logon sequence. At this point the VPN/SSL session has been established, the user ID and password have been authenticated, and the Digital Signature has been confirmed. This event initiates the ERDS Security Process download.

iv. **Submit Digitized (e)** – An event received from an Authorized Submitter's workstation signaling readiness to start the thread of assembly and submission (sending) of the digitized document to the County Recorder.

v. **Assemble Digitized Record** – The process of verifying and combining the components (digitized image, index, etc.) into a message to be sent to the County Recorder.

vi. **Submit Digital (e)** – An event received from an Authorized Submitter's workstation signaling readiness to start the thread of submission and sending of a digital document to County Recorder.

vii. **Assemble Digital Record** – The process of selection and verification of a digital document to be sent as a message to the County Recorder.

viii. **Run Message Authentication (Hash)** – The process that executes a "hash" algorithm to calculate some number to assure authentic origin of the message. The number shall be sent with the message, and used by the receiver (County Recorder) to verify authenticity and integrity of the message.

ix. **Sign with Certificate** – The process of encrypting the message with a key (public or private) to indicate the source (originator) of the message.

x. **Send to Recorder** – The process of setting the message in a format suitable for transmission over the Internet and submitting it as a REQUEST type of message to a web server of a County Recorder.

xi. **Instrument Sent (REQUEST) (e)** – The event ending the process thread of submitting the document.

xii. **Acknowledge Generated (RESPONSE) (e)** – The event signaling the response of the web server.

xiii. **Receive Acknowledge** – The process of receiving the response of the web server and separating the acknowledge message.

xiv. **Confirm Sender** – The process of decrypting the message received to assure the identity of the sender.

xv. **Authenticate Message** – The process utilizing the "hash" value received with the message to validate that the received digitized or digital file was not altered during transmission.

xvi. **Separate Components** – The process of extracting the components of the message and preparing them for further processing.

xvii. **Ready to Process (e)** – A signal to the processes of the Authorized Submitter about the received components. This is the Recorder's response to the Authorized Submitter indicating results of recordation.

Note: Processes and events i -xvii. **(Figure 2)** define the boundary of the ERDS on the Authorized Submitter side of the system. The County Recorder side and processes and event identified as I. – XIV are shown in **Figure 3.**

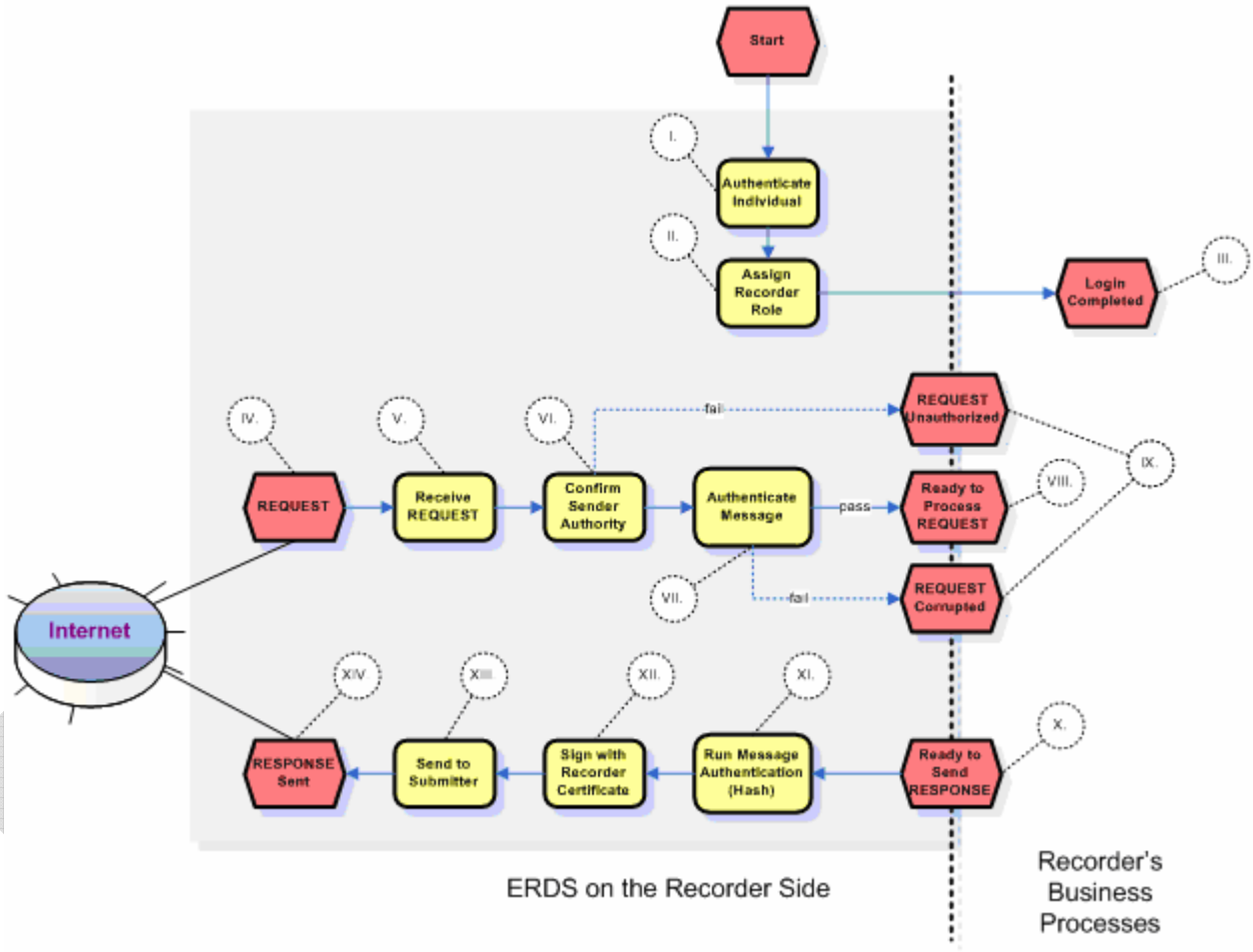

Figure 3 - **ERDS Security Processes on the Recorder's Side.**

I. **Authenticate Individual –** same as i.

II. **Assign Recorder Role –** A person identified by the ERDS is assigned a specific role in the recordation process. The role provides specific privileges, dictating the level of access to the ERDS, and permissions to examine and record digital, digitized, or both documents/instruments, and communicate the results with the Authorized Submitter.

III. **Login Completed (e) –** same as iii.

IV. **REQUEST (e) –**This event signals the beginning of the thread to read and validate the incoming message on the County Recorder's side of the ERDS.

V. **Receive REQUEST –** The process of accepting the request and extracting the message from the Internet transport protocol.

VI. **Confirm Sender Authority –** same as xiv.

VII. **Authenticate Message –** same as xv.

VIII. **Ready to Process REQUEST (e) –** same as xvii.

IX. **REQUEST Unauthorized** or **REQUEST Corrupted (e)** – Events initiating process threads of repudiation of the incoming message.

X. **Ready to Send RESPONSE (e) –** An event signaling to the ERDS Security Processes that the message was processed, and the responding message was prepared and is ready to be sent to the Authorized Submitter.

XI. **Run Message Authentication (Hash) –** Analogous to the viii. The process of the Authorized Submitter, but run on the ERDS Server.

XII. **Sign with Recorder Certificate –** Analogous to the ix. The process of the Authorized Submitter, but run on the ERDS Server.

XIII. **Send to Authorized Submitter –** The process of packing the encrypted message into Internet transport protocol, addressing it to the Authorized Submitter, and sending it via Internet.

XIV. **RESPONSE Sent (e) –** The event signaling the end of the RESPONSE thread.

Note: Processes and events i- xvii, and I - XIV, as specified above, and implemented as software modules identify mandatory software boundaries of the ERDS Program.

4 DATA EXCHANGE ARCHITECTURE

This section defines the required message structures for ERDS documents.

4.1 BACKGROUND: MODELS OF ELECTRONIC RECORDATION

Following are brief definitions of the existing three models of electronic recordation. The definitions are based on concepts suggested by Fannie Mae, used in Minnesota's ERERTF program[1], and are emerging as a standard vocabulary in the industry[2]. These definitions are presented here only as a frame of reference. The ERDS Program shall use these to correlate its definitions of Digitized/Digital documents with these models.

Model 1: Digitized image replaces paper document – At this level the recording process is enhanced by replacing paper documents with electronic images. The Authorized Submitter shall transmit an electronic image of the document to be recorded to the County Recorder. Once received, the County Recorder Examiner reviews the information on the image and manually enters indexing information into the recording system. The Authorized Submitter always retains the original document. However, the image becomes the document of record. Efficiencies are achieved at the county by eliminating scanning and mailing processes.

Model 2: Digitized image with electronic signature and indexing information – At this level the electronic documents prepared by an Authorized Submitter are converted to digitized images (TIFF images). The preparation process is further enhanced by inclusion of indexing data elements and electronic signatures. The Authorized Submitter transmits a digitized image of an originating electronic document with appropriate indexing information about the content of the document, if required - Electronic Signature of the Notary, authentication provision, and is wrapped with electronic signature of the Instrument's Authorized Submitter. Once received, the County Recorder Examiner reviews the information and uses the data provided as indexing information for the recordation. Electronic images become the documents of record and are returned to the Authorized Submitter. Additional efficiency is gained at this level by eliminating some data entry.

Model 3: Digital or fully electronic – At this level recordation can be completed without manual intervention. The Authorized Submitter creates an XML based electronic document that includes both data and presentation information (XML). This document is wrapped with a digital signature and shall also include digitized signatures. Once received, the County Recorder's systems shall validate document integrity and proceed with automated indexing. Business rules shall be used to validate the recordation. The image of the document shall be generated and shall serve as a document of record. Receipt and recording information is returned to the Authorized Submitter electronically. This level

[1] Electronic Real Estate Recording Task Force program for State of Minnesota, http://www.commissions.leg.state.mn.us/lcc/erertf.htm

[2] See presentation http://www.spers.org/spers/media/ElectronicRecordingandElectronicNotarization.PPT

provides the greatest efficiency improvement since no manual intervention is required and processing time is greatly reduced.

The ERDS Program is a "hybrid" of Model 2 and Model 3 mentioned above. It is using Model 2 for digitized documents (any instrument may be submitted for recordation in this format) and Model 3 [3] for digital documents of the following nature:

1. Instruments of reconveyance
2. Substitution of trustee
3. Assignment of Deed of Trust

Model 1 shall not be used for ERDS. It does not provide adequate security and integrity for the digitized documents. In addition, it does not provide for the authentication of the authorized submitter, thereby not providing for the non-repudiation of a document.

[3] See Gov. Code sec. 27397.5, (a).

4.2 ERDS DEFINITIONS OF DIGITIZED/DIGITAL INSTRUMENTS

4.2.1 Digitized Instrument

The ERDS Program defines a Digitized Instrument as a computer-generated record containing a digitized image of an original paper document scanned during the record's preparation or a digitized image of an originating electronic document with appropriate indexing information about the content of the document, if required - Electronic Signature of the Notary[4], authentication provision[5], and is wrapped with electronic signature of the Instrument's Authorized Submitter. This definition coincides with the accepted Electronic Recordation Model 2.

The structure of the Digitized Instrument as adopted by the ERDS Program is depicted in **Figure 4**. This structure is transmitted by an Authorized Submitter[6] to an ERDS of a County Recorder.

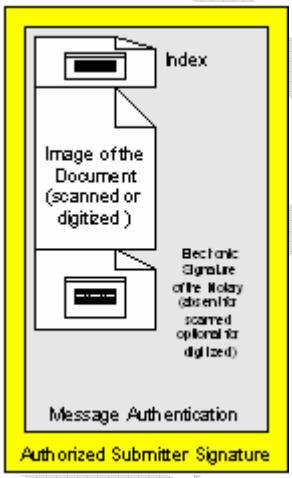

Figure 4 - ERDS Structure of Digitized Instrument

The Electronic Signature of Notary appears only on instrument images digitized from electronic documents, if business rules require notarization of grantor/grantee signatures.

The structure is a payload (Index, Document Image, Electronic Signature of the Notary - optional) in a Message Authentication envelope, wrapped with the electronic signature of the Authorized Submitter.

[4] County may elect Electronic Signature of the Notary, Gov. Code 27391, (e).
[5] See more on that in "Security Requirements" chapter *(preliminary name!).*
[6] Specifics about the Authorized Submitter's role are delineated in "Submit Instrument, Digitized" chapter in this document.

4.2.2 Digital Instrument

The ERDS Program defines a Digital Instrument as a complex XHTML document (XML content + HTML format) created electronically instead of a digitized image. The structure of the Digital Instrument consists of the XHTML file; Electronic Signature of the Notary and electronic stamp, if required by the County Recorder's business rules (optional); message authentication provision[7]; and is also wrapped with the electronic signature of the Instrument's Authorized Submitter. This definition coincides with the accepted Electronic Recordation Model 3 cited above.

The Index information is automatically extracted from the XML content of the incoming message by a County Recorder Examiner allowing automatic indexing and recordation. Seven mandatory Index fields described in the "Index & Electronic Signature of the Notary" section have to be tagged in the XML content of the document as separate elements.

The structure of a Digital Instrument as adopted by the ERDS Program is depicted in **Figure 5**. This structure is transmitted by an Authorized Submitter to an ERDS of a County Recorder[8].

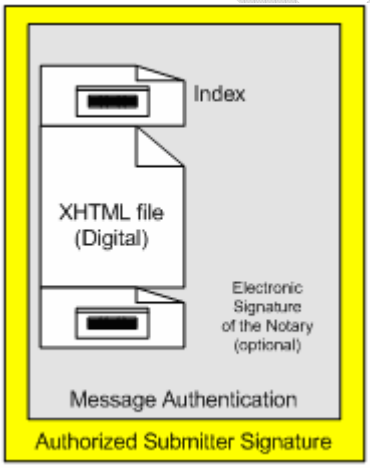

Figure 5 - ERDS Structure of Digital Instrument

[7] See more on that in "Security Requirements" chapter.
[8] See more on the role of Authorized Submitter of digital documents in "Submit Instrument, Digital" chapter.

4.3 DIGITIZED IMAGE STANDARDS

In the case of a Digitized Instruments generated from paper documents, the size of the documents should be restricted to a Letter (8.5”x11”) or Legal (8.5”x14”).

Digitized images may be black and white, tonal, or color and depending on the selection by the county will impact capacity.

The ERDS Program restricts image formats for documents to TIFF[9] and/or PDF[10] with resolutions not less than 200 pixels per inch for scanning paper images.

[9] Acronym for tagged image file format, one of the most widely supported file formats for storing bit-mapped images on personal computers (both PCs and Macintosh computers). Other popular formats are BMP and PCX. TIFF graphics can be any resolution, and they can be black and white, gray-scaled, or color.

[10] Short (acronym) for Portable Document Format, a file format developed by Adobe Systems. PDF captures formatting information from a variety of desktop publishing applications, making it possible to send formatted documents and have them appear on the recipient's monitor or printer as they were intended.

4.4 INDEX & ELECTRONIC SIGNATURE OF THE NOTARY

Existing California [11] law requires the presence of the following fields for recorded documents:

Field	Description	Origin
Date Filed	Date this instrument was filed for recordation	County ERDS (Recorder) upon successful reception of the instrument from an Authorized Submitter
Grantor	Full name of a person or organization playing the role of grantor/defendant/first party for this Instrument	Authorized Submitter
Grantee	Full name of a person or organization playing role of the grantee/plaintiff/second party for this Instrument	Authorized Submitter
Title	Title of the Instrument	Authorized Submitter
Document Number	Unique document number that was assigned to the Instrument at time of recordation	County Recorder
Book	Volume in which the record of the instrument was made by the Recorder	County Recorder
Page	Page on which the record of instrument was made by the Recorder	County Recorder

[11] Gov. Code 27257

The following fields shall be in the Electronic Signature of the Notary of a payload if a County Recorder implements an Electronic Signature of the Notary for the ERDS (all fields are mandatory, but data may not be present)[12]:

1. The name of the notary.
2. The words ‘‘Notary Public.’’
3. The name of the county where the bond and oath of office of the notary are filed.
4. The sequential identification number assigned to the notary, if any.
5. The sequential identification number assigned to the manufacturer or vendor of the notary’s physical and/or electronic seal, if any.

4.5 TRANSMISSION PROTOCOL

The ERDS Program shall rely on the public Internet for transmission of Instruments of interest. Every ERDS shall use Virtual Private Network (VPN) or SSL V3/TLS protocols utilizing NIST-approved algorithms. Authorized Submitter’s workstation sends a generalized REQUEST, a County ERDS (WEB Server) answers with a RESPONSE. The pair REQUEST-RESPONSE describes an atomic[13], asynchronous[14] Application Transaction. To assure a high level of independence, the ERDS Program adopts XML to carry the payload (case of digitized image should be a part of XML) as a mandatory format for all application messages.

4.6 TRANSACTION PROTOCOL

This section describes mandatory requirements for the application transaction protocol. This section deals with only one major transaction:

- **Submit Instrument** – An Authorized Submitter sends a created Instrument (scanning image, or creating electronic document, typing the relevant Index values[15]) to a County ERDS, which responds back with a confirmation/rejection message.

The transactions shall have different formats for Digitized or Digital Instruments. Details of these differences are elaborated in the following sections.

[12] Gov. Code 27391, (e).
[13] Atomic – means any single REQUEST has all information sufficient and necessary for executing the corresponding RESPONSE.
[14] Asynchronous in this context means independent upon the previous order (stateless) of the communication session between Authorized Submitter and a County Recorder ERDS.
[15] See section 3.4 in this document for details.

4.6.1 Submit Instrument, Digitized

Only an Authorized Submitter in the role of Secure Access shall have permission to build and submit these transactions. The process of role assignments is done during the log-in thread of processes on an Authorized Submitter's workstation.[16] Any type of document/instrument may be submitted for recordation in this transaction. The Authorized Submitter in this role shall assemble the message from the prepared image(s). This activity is shall be governed by the County Recorders recordation process.

Transaction messages for Digitized Instruments are depicted in **Figure 6**.

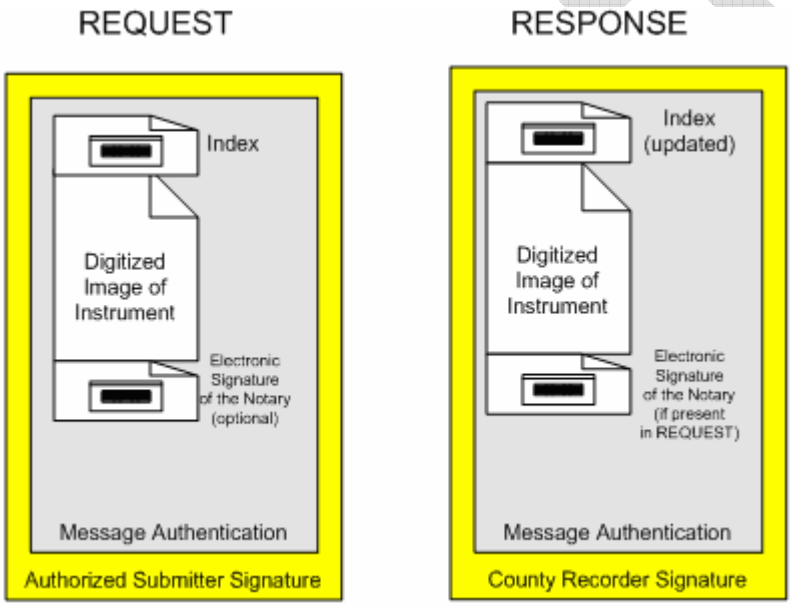

Figure 6 - 'Submit Instrument' Transaction for Digitized Instrument

The Authorized Submitter initiates the REQUEST message electronically encrypting it with his/her private key (Signature envelope in the picture).

The County Recorder Examiner[17] returns the Instrument with the recordation information added to the Index, and, may record the document image change by 'stamping' as required by county recordation process, encrypted with the County Recorder's Signature to the Authorized Submitter.

[16] More details on this are presented in "ERDS Boundary", processes (i.)-(ii.)
[17] See "Authorization Standard" in "System Access Control" chapter.

4.6.2 Submit Instrument, Digital

Submission of a Digital Instrument is done by an Authorized Submitter in the role of Authorized Access[18] from the Authorized Submitter's workstation. An Authorized Submitter in this role shall build the message from the previously prepared digital document, and also shall encrypt it with a key. Only three types of documents shall be submitted in this transaction:

- Instruments of reconveyance
- Substitution of trustee
- Assignment of deed of trust

In the case of ERDS using Digital Instruments, the equivalent transaction messages are presented in **Figure 7.**

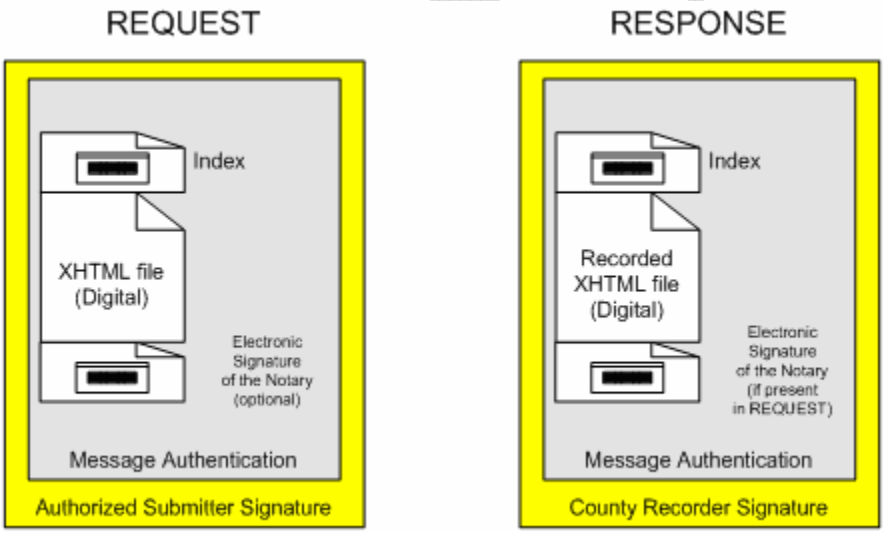

Figure 7 - 'Submit Instrument' Transaction for Digital Instrument

[18] The Secure Access role shall also assume responsibilities of the Authorized Access role.

4.7 REQUIREMENTS

1. An Authorized Submitter workstation shall exchange data with the ERDS in the form of data messages with the County Recorder's ERDS using the public Internet.
2. Communication sessions shall be initiated by Authorized Submitter's workstation.
3. Sessions shall be protected as described in the security requirements section of this document.
4. A session shall consist of one or more REQUEST-RESPONSE actions (the Authorized Subscriber workstation sends a REQUEST, ERDS provides appropriate RESPONSE).
5. Detailed protocols of sessions shall be developed by the County Recorder with an internal development team or a Certified Software Vendor to reflect specific business practices of recordation by the county, but shall include a mandatory transaction: Submit Instrument.
6. Messages shall comprise data exchange between an Authorized Submitter and the ERDS shall be formatted as XML payloads with images of digitized instruments.
7. XML Payloads should include the mandatory index structure for each instrument consisting of the seven fields that are listed in section 4.4 of this document.
8. If the County Recorder decides to implement an Electronic Signature of the Notary, the following elements should be added to the payload:
    a. The name of the notary.
    b. The words ''Notary Public.''
    c. The name of the county where the bond and oath of office of the notary are filed.
    d. The sequential identification number assigned to the notary, if any.
    e. The sequential identification number assigned to the manufacturer or vendor of the notary's physical and/or electronic seal, if any.
9. Digital Instruments shall be exchanged using XHTML protocol.
10. Detailed XML Schemas for each message (Digital/Digitized) shall be developed by the County Recorder and shall be submitted to the ERDS Program as a part of the ERDS Certification process.
11. Messages used to transport Digital/Digitized Instruments shall be wrapped in a message authentication envelope (secure hash algorithm)[19].

[19] See "Security Requirements" for more details.

5 SECURITY REQUIREMENTS

5.1 TECHNICAL SECURITY

Technical security controls protect the integrity of system configurations and the information contained in submitted documents. Administrative controls provide management guidance. Physical security controls protect the integrity of installed hardware by limiting physical access to systems. Technical controls protect installed software, data, and configurations by limiting logical access to systems. This document sets the baseline requirements and standards for these technical security controls.

5.1.1 Conceptual Overview

ERDS systems shall protect data, both in storage and transmission, provide mechanisms to detect unauthorized changes and verify the integrity of information contained in documents.

5.1.1.1 Major Components

A conceptual diagram showing the major components of a typical network that supports ERDS is given in **Figure 8**. Each network component is identified and defined in relation to ERDS components.

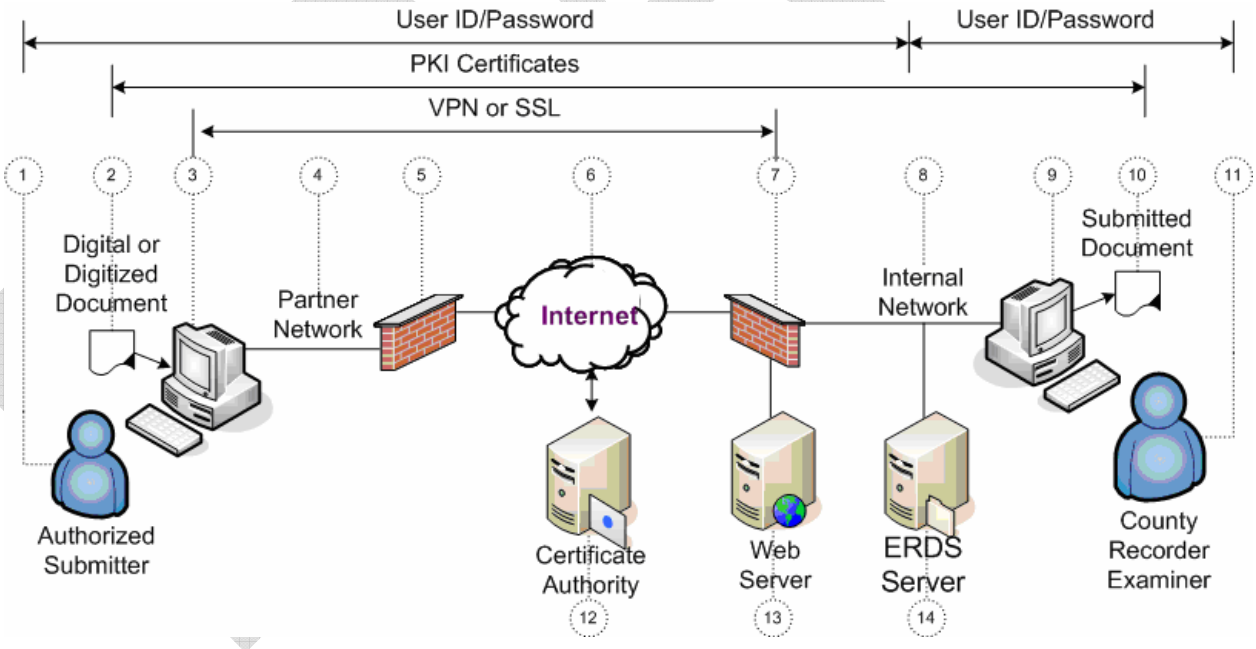

Figure 8 - Conceptual Infrastructure

Major components supporting ERDS operations are:

1. **Authorized Submitter -** An entity of the Industry (Title Insurer, Title Company, Lending Institution) or Government (Local, State, Federal Agency) that is a party to a contract with a County Recorder to use an ERDS as a tool to electronically submit digital/digitized instruments for recordation.
2. **Digital or Digitized Document -** Documents prepared for submission.
3. **Partner Workstation -** Contains or downloads software necessary for ERDS functions.
4. **Partner Network -** Internal network of the Authorized Submitter organization. Use of Partner Networks for ERDS shall comply with the ERDS Baseline Requirements and Technology Standards.
5. **Partner Perimeter -** Perimeter security systems of Authorized Submitter organizations can include multiple security devices, such as firewalls, intrusion detection and/or prevention systems, virtual private network gateways, and other devices. Use of a Partner Perimeter for ERDS shall comply with the ERDS Baseline Requirements and Technology Standards.
6. **The Internet -** Defined to include all other networks that are neither internal nor partner networks. Use of the Internet for ERDS shall comply with the ERDS Baseline Requirements and Technology Standards.
7. **County Perimeter -** Perimeter security systems of counties shall include security devices configured to protect ERDS components from unauthorized activity occurring on internal or external operations. As a minimum, systems shall include a firewall and intrusion detection and/or prevention systems. Connections to ERDS made via virtual private networks shall still come under the controls provided by the perimeter security systems.
8. **Internal Network -** Network used by County Recorder.
9. **County Workstation -** Contains or downloads software necessary for ERDS functions.
10. **Submitted Documents -** Documents retrieved from ERDS by a County Recorder.
11. **County Recorder Examiner -** A role in the County Recorder's office authorized to review documents submitted for recordation.
12. **Certificate Authority -** The certificate authority issues digital certificates for the purpose of establishing SSL sessions between Authorized Submitters and the County Recorder. The Certificate Authority also validates digital certificates presented as proof of identity.
13. **Web Server -** County server that acts as the interface to Authorized Submitters. Login occurs at the web server.
14. **ERDS Server -** Receives submitted documents from the web server. Sends processed documents back to the web server.

5.1.1.2 Access Process

An ERDS user shall follow this sequence of events:

1. Prior to accessing ERDS, a user logs in at their assigned workstation. The established login sequence to the network takes place.
2. Upon successful login to the partner network, the user starts a browser session.
3. The user surfs to the County Recorder website.
4. The user clicks a link to the County Recorder ERDS page.
5. ERDS initiates a VPN/SSL session between the County Recorder and the Authorized Submitter's workstation.
6. Once the VPN/SSL session is established, the user is prompted for a user ID and password.
7. If the user ID and password are authenticated, the user is prompted to confirm their identity using a digital signature.
8. If the digital signature is confirmed, the user is recognized as an Authorized Submitter.
9. The ERDS application starts.

5.1.2 Access Control

ERDS shall apply a combination of system, network and data security mechanisms. The integrity of the system shall be protected using role-based access control mechanisms.

5.1.2.1 Identification Standard

1. Each Authorized Submitter shall be uniquely identified.
2. Shared credentials are prohibited.
3. The Authorized Submitter's name shall either be a verified name or a pseudonym.[20]

5.1.2.2 Authentication Standard

1. Authentication shall employ at least two of the three factors defined in NIST Special Publication 800-63 http://csrc.nst.gov/publications/nistpubs/index.html. Two-factor authentication is commonly referred to as "strong authentication".
2. Each person having access to ERDS shall authenticate using a digital certificate in combination with either a user ID/password or biometric identifier.
3. Authentication assurance shall meet Level 3 or higher, as defined in NIST SP 800-63, Section 8.2. "Authentication Mechanism Requirements"
4. Any of the token methods described in NIST SP 800-63, Section 6, may be used provided authentication assurance Level 3 is achieved.

[20] NIST SP 800-63, Version 1.0.1, "Electronic Authentication Guideline", Sep. 2004, pg 10.

5.1.2.3 Authorization Standard

Access shall be controlled using a role-based access control system. The County Recorder shall control the assignment of roles to individuals.

The following roles shall be defined:

1. **Secure Access -** Authorized Submitters who are authorized to submit digital and digitized documents (Secure Access) to the County Recorder.
2. **Authorized Access -** Authorized Submitters who are authorized to submit digital documents (Authorized Access) to the County Recorder.
3. **County Recorder Examiner -** Authorized to review documents submitted for recording. County Recorder Examiners are authorized to review, reject, stamp and record, and return documents to Authorized Submitters.
4. **Computer Security Auditor -** Authorized to review transaction logs and conduct tests on computer security mechanisms.
5. **Developer -** Authorized to develop application software, but deployment is limited to the test environment.
6. **Deployer -** Authorized to deploy approved application software to production systems.
7. **System Administrator -** Authorized to configure hardware and operating system software.
8. **Security Administrator -** Authorized to configure accounts, assign roles, and issue credentials.

5.1.2.4 Accounting Standard

The following Auditable Events shall be logged for analysis, audits and local inspections. Logs must be retained for a period of two years:

No.	Event	Pertains to:	Logged at or by:
1.	Login, both successes and failures.	a. ERDS Accounts b. System Accounts c. Network Accounts	a. ERDS Server b. County Recorder workstation, ERDS Server c. Network authentication server.
2.	Session, both start and end.	ERDS Sessions	Web Server and/or network authentication server.
3.	Document submission.	ERDS Server	ERDS Server
4.	Document return, whether recorded or rejected.	ERDS Server	ERDS Server
5.	Session time-outs (e.g. inactive in excess of 15 minutes).	Web Server	Web Server
6.	Unauthorized privilege use (e.g. unauthorized person attempting to access protected storage areas or an authorized user attempting to access unprotected areas).	a. County Recorder workstation b. ERDS Server c. Web Server	County Recorder workstation, ERDS Server, Web Server and/or network authorization server.
7.	Use of expired or revoked credentials.	a. ERDS Accounts. b. County Recorder workstation, ERDS Server, Web Server or network accounts.	a. ERDS Server b. County Recorder workstation, ERDS Server, Web Server and/or network authentication server.
8.	User account creation, modification, deletion, suspension, termination or revocation.	ERDS Server (or network authentication and authorization servers)	ERDS Server (or network authentication and authorization servers)
9.	Unescorted visitor access to protected systems.	County Recorder workstation, ERDS Server, Web Server	County Recorder and/or server rooms.
10.	Software configuration changes. Document all software installed on workstations and servers since the most recent audit.	County Recorder workstation, ERDS Server, Web Server	County Recorder
11.	Hardware configuration changes. Document all hardware installed in, or attached to workstations and server systems	County Recorder workstation, ERDS Server, Web Server	County Recorder
12.	Network configuration changes. Document all configuration changes made to the network, including hardware, software, protocols, and routing.	Network segments connecting County Recorder workstation, ERDS Server, and Web Server	County Recorder

Auditable events shall be logged for all ERDS sessions and transactions processed by County Recorder workstations, ERDS Server(s), Web Server(s) and network authentication and authorization servers.

To maintain audit trails, audit logs shall be off-loaded to non-volatile storage. Auditable events shall never overwrite other logged events. The ERDS Server shall not accept documents if:

1. Transactions cannot be logged, or
2. Audit logs consume 95% of allocated audit storage and cannot be off-loaded.

The County Recorder shall be notified of that an operational error has occurred when ERDS Server audit logs cannot be off-loaded to non-volatile storage.

5.1.3 Document Security

Whether digitized or digital, document security shall be applied equally.

5.1.3.1 Document Control

Authorized Submitters shall assure submitted documents, digital or digitized, do not contain any components that draw data or images from sources external to the document including, but not limited to, the following:

1. Viruses
2. Worms
3. Trojan Horses
4. Spyware
5. Adware
6. ActiveX components
7. JavaScript
8. Java components
9. HTML encoded hyperlinks
10. Any other executable software

County Recorders shall ensure that all county workstations designated to process submitted documents receive anti-malware updates to maintain currency with the most up-to-date releases. Such updates shall occur prior to processing documents; however, County Recorders shall process unencrypted documents known to have been scanned using up-to-date anti-malware software.

5.1.3.2 Submitting Documents

Once materials are prepared and collected, an Authorized Submitter logs into the ERDS and begins the submission process.

The Authorized Submitter's workstation collects the index, document image or file, and the Electronic Signature of the Notary into a single record structure. The record structure is hashed using the secure hashing standard, as defined in section 5.1.3.2.4 of this document. The hash value is signed using the private key of the Authorized Submitter -- creating the hashed message authentication code, or digital signature, of the Authorized Submitter (**Figure 9**).

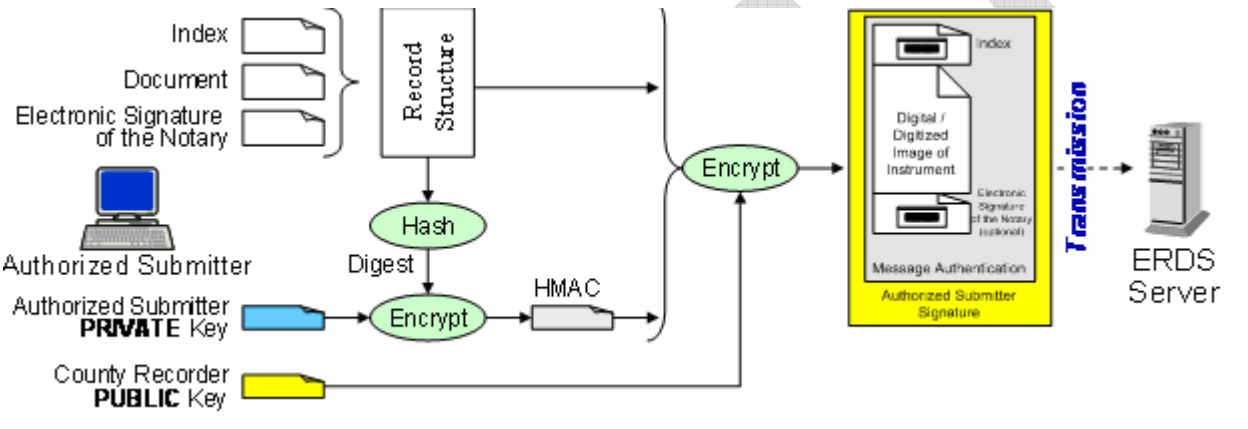

Figure 9 - ERDS Document Submittal (Send)

Once the Authorized Submitter is satisfied that the record is ready for recording, the record structure and digital signature of the Authorized Submitter are encrypted using the public key of the County Recorder and the encrypted package is transmitted.

Transmitted documents are relayed through the web server to the internal ERDS server. The web server acts as a proxy between the Authorized Submitter and the ERDS server. There shall be no capability to directly log into the ERDS server from the Internet.

5.1.3.2.1 Retrieving Documents

At the County Recorder, the ERDS server receives each encrypted package and temporarily stores it in a controlled file location. Although protected by encryption, role-based access controls determine where files are stored and which users can retrieve them. County Recorder Examiners are authorized to retrieve stored documents for review (**Figure 10**).

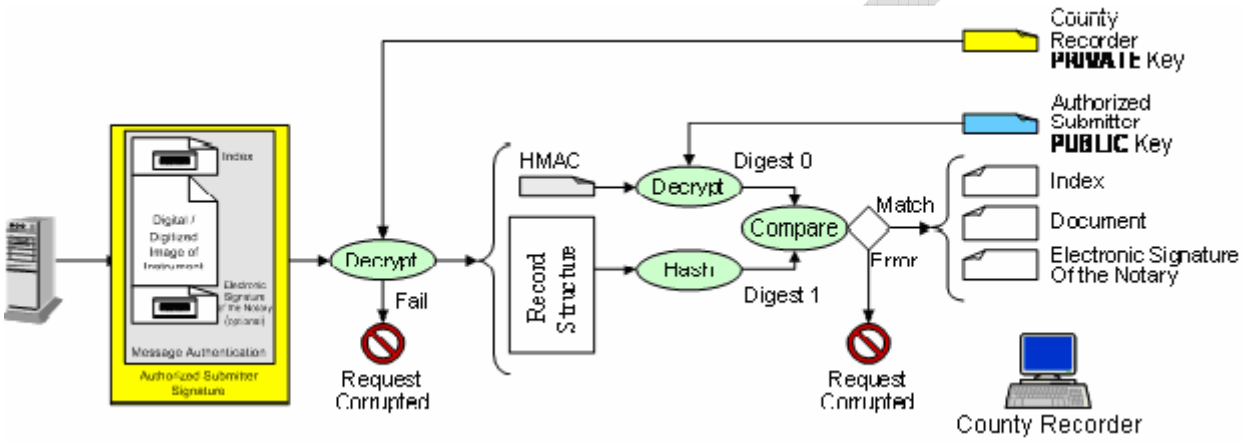

Figure 10 - ERDS Document Submittal (Retrieve)

Until a County Recorder Examiner reviews a document, the document shall remain secured in storage. Encryption and role-based access control shall protect the confidentiality and integrity of documents until a County Recorder Examiner retrieves and opens a document for review.

In the process of retrieving documents, the ERDS decrypts and authenticates that the document has not been corrupted. The County Recorder's Private-key is used to decrypt the stored document. If the decryption fails, the document cannot be read. If the decryption succeeds, the document structure and the digital signature of the Authorized Submitter become readable.

When a document is retrieved for review, the ERDS shall validate the digital signature of the Authorized Submitter accompanying that document. Validation ensures (a) the document was sent from an Authorized Submitter, and (b) the document was not tampered with, either in transit or storage.

Decryption failure can be attributed to simple file corruption, but it can also indicate tampering. Validation failure can also indicate tampering. If either decryption or validation fails, the document shall be returned to the Authorized Submitter for resubmission.

Once the document has been validated and accepted by the County Recorder, a copy of the original record structure sent by the Authorized Submitter must be retained at least two years.

5.1.3.2.2 Reviewing Documents

If the document can be decrypted and validated, the County Recorder Examiner proceeds through the process of reviewing the document for recording according to the recordation process established by the County Recorder.

5.1.3.2.3 Returning Documents

Once a County Recorder Examiner accepts or rejects a document, the process of returning the document to the Authorized Submitter is the reverse of the submittal process. The primary difference is in the use of public and private keys.

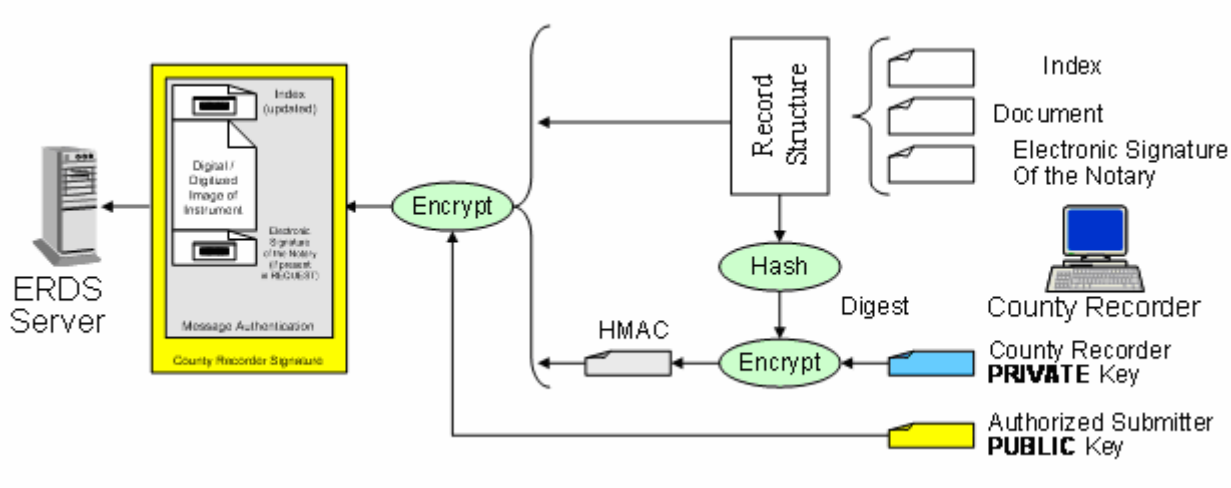

Figure 11 - ERDS Document Return (Send)

In returning the document to the Authorized Submitter, ERDS hashes and encrypts the document to protect it in storage and transmission. A diagram of the County Recorder return process is shown in **Figure 11**.

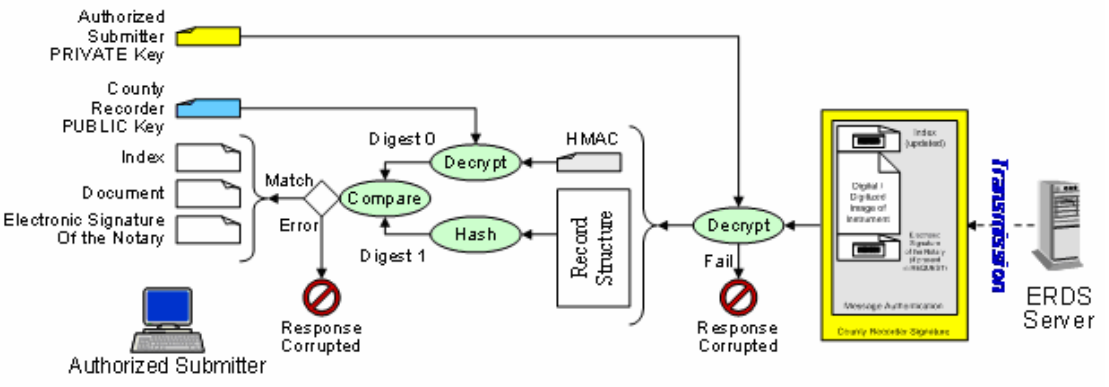

Figure 12 - ERDS Document Return (Receive)

In receiving a document from the County Recorder Examiner, ERDS decrypts and validates the returned document for use by an Authorized Submitter. A diagram of the Authorized Submitter return process is shown in **Figure 12**.

5.1.3.2.4 Document Confidentiality and Integrity

Although a VPN or SSL/TLS connection is an effective means of protecting documents in transit, additional precautions shall be taken to protect documents in storage. Participants shall employ both role-based access control mechanisms and encryption to protect documents in storage.

Document access control shall be strictly enforced after entering a document into ERDS. Document access shall be based on the standards defined in section 5.1.2.3.

Document confidentiality shall be maintained using public key cryptography in a Public Key Infrastructure (PKI). The PKI shall be the responsibility of by the County Recorder and shall be used for encrypting documents in transit and storage. Digital certificates shall be issued to all individuals authorized to submit documents using ERDS.

Capacity Note: To prevent unnecessary consumption of CPU throughput, encrypted documents shall remain encrypted for the entire process between Authorized Submitter and County Recorder.

The Secure Hash Standard, described in FIPS 180-2, shall be used to protect the integrity of documents. Documents submitted using ERDS shall be protected using the Keyed-Hash Message Authentication Code (HMAC) described in FIPS 198, March 6, 2002. The Secure Hash Algorithm (SHA) shall be used to generate the Keyed HMAC.

1. The minimum standard algorithm is SHA-224.
2. A keyed-HMAC shall be generated as soon as the digitized or digital document, including index and/or the optional notary electronic signature are introduced into ERDS.

5.1.4 Application Security

Major components shall be physically and logically separate.

Permissible connections are:

1. Authorized Submitter workstation to/from Web Server.
2. Web Server to/from ERDS Server.
3. ERDS Server to/from County Recorder workstation.

5.1.5 Server Security

5.1.5.1 Server Configurations

The ERDS web server, which resides outside the County Recorder network, is to be solely dedicated to the ERDS environment and must not provide any other services or functionality. No direct logins to the ERDS server via the internet, bypassing the ERDS Web server, are allowed. ERDS servers that reside inside the County Recorder network, are allowed to be utilized for multiple services/functionalities.

5.1.5.1.1 Web Server

Web servers exposed to the Internet are most vulnerable to external attack, so strict access control, system hardening and robust network security is required.

Web servers shall:

1. Provide the public interface to ERDS.
2. Establish SSL sessions.
3. Authenticate SSL credentials.
4. Transfer and or relay ERDS requests received via authenticated SSL sessions to the ERDS Server.

5.1.5.1.2 ERDS Server

The ERDS server shall house all ERDS functionality except for enterprise services that the County Recorder Examiner has provided in their infrastructure. The ERDS server shall:

1. Run ERDS software
2. Store ERDS files
3. Authenticate ERDS credentials
4. Control ERDS access based on assigned roles
5. Log ERDS transactions

The ERDS server shall interoperate with the web server when establishing secure connections with Authorized Submitters; however, the ERDS server is the primary source of functionality for ERDS. County Recorder Examiners using ERDS shall receive all ERDS functionality from the ERDS Server.

The ERDS server shall be contained on a segment of the internal network that prevents unauthorized access from internal network users.

The County Recorder shall select checklists for hardening servers, workstations, applications and networks through the "NIST Security Configuration Checklists Program for IT Products". Available checklists are at: http://csrc.nist.gov/checklists. Guidance for selection is available in NIST Special Publication 800-70, "Security Configuration Checklists Program for IT Products – Guidance for Checklists Users and Developers".

Checklists may be selected from:

1. NIST Information Technology Security Practices, Checklists and Implementation Guides - http://csrc.nist.gov/pcig/cig.html
2. NSA Security Configuration Guides - http://www.nsa.gov/snac/index.cfm?MenuID=scg10.3.1
3. Center for Internet Security Benchmarks and Scoring Tools - http://www.cisecurity.org/bench.html

County Recorders shall select checklists based on the technologies used for implementing ERDS locally. County Recorders may add checklist items and tailor checklists to reflect local conditions; however, checklist items must not be removed. Checklists modified by a County Recorder shall be submitted to the Attorney General for use by any County utilizing ERDS.

Note: Results from the checklists may or may not be attributed to environmental or operational factors and must be considered when reviewing the output from the checklist tools. Justification will be required for any items that are not remedied as a result of the checklist recommendations.

At a minimum, the following checklists (or a corresponding checklist available from NSA or CIS) shall be used as the basis for hardening ERDS implementations:

1. Operating System STIG for the implemented operating system
2. Access Control STIG (DRAFT) Version 1, Release 0 (454 KB) - http://csrc.nist.gov/pcig/STIGs/AccessControlSTIGV1R0_DRAFT.doc
3. Application Security Checklist Version 2, Release 1.7 (1.59 MB) - http://csrc.nist.gov/pcig/CHECKLISTS/app-security-checklist-v2r17-19aug05.doc
4. Application Services STIG Version 1, Release 0.1 (921 KB) - http://csrc.nist.gov/pcig/STIGs/eds-application-services-stig-final-to16.doc
5. Desktop Application STIG (714 KB) - http://csrc.nist.gov/pcig/STIGs/Desktop-Application-STIG-V2R1.pdf
6. Desktop Application Security Checklist Version 1, Release 1.10 (789 KB) - http://csrc.nist.gov/pcig/CHECKLISTS/desktop_app_checklist_v1r110.zip
7. IP WAN Checklist Version 2.3 (423 KB) - http://csrc.nist.gov/pcig/CHECKLISTS/ipwan-checklist-v2r3.pdf
8. Network STIG Draft Version 6 Release 3 (2,184 KB) - http://csrc.nist.gov/pcig/STIGs/network-stig-v6r3.pdf
9. Network Infrastructure STIG (1,500 KB) - http://csrc.nist.gov/pcig/STIGs/NETWORK-STIG-V5R2%209-29-2003FINAL.doc
10. Network Infrastructure Security Checklist Version 5 Release 2.4 (1,483 KB) - http://csrc.nist.gov/pcig/CHECKLISTS/network-checklist-v5r2_4-042005.doc
11. Secure Remote Computing STIG Version 1, Release 2 (908 KB) - http://csrc.nist.gov/pcig/STIGs/src-stig-v1r2.pdf
12. Web Server Checklist and Procedures Version 5.0, Release 1 (1.54 MB) - http://csrc.nist.gov/pcig/CHECKLISTS/web-checklist-procedures-080505.zip
13. Web Server STIG (1,672 KB) - http://csrc.nist.gov/pcig/STIGs/Web-STIG-V5R1.pdf
14. Web Servers and Browser Security Configuration Guide NSA (3.05 MB) - http://csrc.nist.gov/pcig/CHECKLISTS/webs_securityguides-nsa.zip

Note: For a suggested network configuration, refer to NIST Special Publication 800-70, "Security Configuration Checklists Program for IT Products – Guidance for Checklists Users and Developers". In NIST SP 800-70, Figure 3-3 on page 32 illustrates a "Typical Specialized Security-Limited Functionality Environment". ERDS can be implemented in a similar fashion by replacing the "Financial Server" shown in the diagram with the "ERDS Server"

5.1.5.2 Enterprise Services

Services that shall be implemented in support of ERDS include authentication services, authorization services, certificate services and key management services. Supporting services may be implemented as part of County Recorder enterprise services or integrated with the ERDS server. These supporting services must comply with the Baseline Requirements & Technology Standards for the Electronic Recording Delivery System (ERDS).

5.1.5.3 Server Hardening

All servers shall be configured to prevent unauthorized access, modification or use, whether publicly accessible or hosted on internal networks.

County Recorders shall document the standard used for "hardening" servers. All servers shall be "hardened" according to one of the following guidelines:

1. NIST Security Configuration Checklist designed for the product. Checklists are available at NIST Security Configuration Checklist Repository at: http://checklists.nist.gov/repository/category.html.
2. Manufacturers recommended guidelines for securing their products to afford the highest level of protection. (Note: Manufacturers recommended guidelines shall be supplemented with the requirements of this document.)
3. Security configuration guidelines available from industry standard sources such as the Computer Emergency Response Team Coordination Center (CERT/CC) or the System and Network Security (SANS) Institute. (Note: Industry hardening guidelines shall be supplemented with the requirements of this document.)

As a minimum, all servers shall:

1. Be "hardened" according to the standard "hardening" guideline identified by the County Recorder.
2. Have a host-based file integrity checking system configured to alert security staff of any system file changes to the ERDS server.
3. Have anti-malware software installed and operating to both protect the server from infection and prevent the distribution of infected files.

5.1.5.4 Server Maintenance

Maintenance for all servers shall include:

1. Anti-malware software updated to maintain currency with the most up-to-date releases.
2. ERDS server logs are to be retained for at least two years.
3. Most up-to-date software patches and hot-fixes applied within seven calendar days of approval by the County Recorder.

5.1.6 Workstation Security

5.1.6.1 Workstation hardening

All workstations shall include:

1. Anti-malware software configured to start on system boot-up.
2. Personal firewall software configured to prevent unauthorized access.
3. Operating System capable of setting privilege levels on files and directories.

5.1.6.2 Workstation Maintenance

Maintenance for all workstations shall include:

1. Anti-malware software updated to maintain currency with the most up-to-date releases.
2. Personal firewall software logs archived and retained for at least two years.
3. Most up-to-date software patches and hot-fixes applied within seven calendar days of approval by the County Recorder.

5.1.7 Network Security

The integrity and reliability of ERDS depends on security measures applied at the network level. ERDS shall use both internal and external networks, including the Internet. ERDS components shall be protected from unrelated activity occurring on either internal or external networks. Networks configurations shall incorporate the common security mechanisms detailed in this document. County Recorders shall take advantage of these security mechanisms in order to develop an efficient and effective overall security program.

5.1.7.1 Perimeter Security

5.1.7.1.1 Perimeter Configurations

Network security controls shall be implemented to prevent malicious and unnecessary traffic from reaching ERDS components. At a minimum:

1. Firewall technology shall:
   a. Employ stateful packet inspection
   b. Limit connection attempts addressed to ERDS components to those ports necessary for ERDS operation; blocking unauthorized port usage.
   c. Be designed and configured to fail “closed” rather than open.
2. Network-based intrusion detection systems (IDS) technology shall identify possible intrusions and if a possible intrusion is detected, send alerts to security staff. Network-based intrusion prevention systems may be used in addition to an IDS.

5.1.7.1.2 Denial of Service Protection

Network security controls shall be equipped and configured to prevent network-based denial of service attacks.

5.1.7.2 Transmission Security

Documents transmitted via any network shall be protected using encryption. Data packets transmitted via internal, external, and partner networks are easily captured and compromised if unencrypted. The standard for encrypting documents in transmission is the Secure Socket Layer (SSL), Version 3.0, also known as Transport Layer Security (TLS), Version 1.0.

Virtual Private Networks as described in NIST SP 800-77 "Guide to IPsec VPNs" (draft), may be used in lieu of SSL-based systems provide they meet the recommendations described in NIST SP 800-63 "Electronic Authentication Guideline" and ERDS Baseline Requirements and Technology Standards.

Prior to beginning any login sequence, a secure channel shall be established in order to protect passwords. As a minimum, an SSL session shall be established before transmitting credentials. Systems employing "basic" or "http" authentication transmit passwords in clear-text are not secure and are unsuitable for ERDS.

Authorized Submitter authentication shall be required to verify that the session is being established from an Authorized Submitter workstation location. Commercially available sources for digital certificates may be used for establishing SSL connections.

5.1.7.2.1 Transmission Integrity

Transmission integrity shall use the same standard defined for document integrity, namely the Secure Hash Standard, described in FIPS 180-2.

5.1.7.2.2 Transmission Confidentiality

Two basic processes that shall be protected during any online session are (1) the login sequence, and (2) document transfer. The protocol required for conducting these operations is Transport Layer Security (TLS), Version 1.0. (TLS V1.0 is also known as Secure Socket Layer, Version 3.0.) As a minimum, 128-bit encryption shall be used to establish TLS sessions. Such sessions shall be established before any user credentials are exchanged. Server-side SSL may be used to establish the initial connection, but client-side SSL shall be established before exchanging user authentication credentials. Once a client-side SSL session is established, Authorized Submitters shall present credentials to the County Recorder Examiner. The client-side SSL session identifies the organization while credentials identify the user. Client-side SSL certificates shall be controlled by the Authorized Submitter organization, but individual user credentials shall be under the control of the County Recorder; either directly or through an independent Certificate Authority.

An independent Certificate Authority shall be another government organization or a commercial organization selected from the list of certification authorities approved by the California Secretary of State.

5.1.8 Media Security

Computer media includes, but is not limited to, fixed disk, removable disk and portable device. Physical access control shall be capable of controlling access to stored files and encryption keys. Access control shall be established through the setting of access control levels. Internal fixed disks and removable media shall be sanitized prior to reallocating ERDS computer equipment or disks for other purposes.

Portable devices include laptops, digital assistants, “flash” or USB drives, key cards, tokens and any other devices capable of transporting confidential data in a compact package.